

Enhanced Security using RSA Algorithm in Cloud Computing

Dr. Sonia Sharma¹, Ashutosh Kumar²

¹Professor & Head, Department of Computer Science and Engineering, MIMIT Malout

²Research Scholar, Department of Computer Science and Engineering, MIMIT Malout

Abstract: The cloud computing has a very important aspect i.e., the security and the quality of service from cloud service providers. However, cloud computing poses many new security challenges which haven't been well investigated. This paper specializes the issues referring to the cloud data storage methods and security within the virtual environment. In this paper, a technique for suggesting data storage and security within the cloud system using combination of public-key and private-key cryptosystem RSA has been implemented [5]. Further, it describes the safety services includes key generation, encryption and decryption within the virtual environment.

Keywords— RSA algorithm, encoding, Cloud Computing, Data Security, Data Decryption

I. Introduction

In the modern distributed era various services offered on the web are a standard hosting system. But within the normal hosting system storage and usage are fixed. Cloud computing imposes a replacement model for computing and the issues like compute, storage, software. A development environment is being provided and the allocation and reallocation of resources is completed wherever storage is needed and virtualized it. It satisfies the on-demand needs of the user. For the organization, the cloud offers data centres to maneuverer their data globally. It removes the usages of local nodes for supporting their data and also cloud supports upgradable resources on the net. Cloud Service Providers maintains Computing resources and data automatically via software [6]. Cloud Computing is that the key thrust in many companies but the key concern is the safety of their data within the cloud. Securing data is sometimes of being vital due to the critical nature of cloud. Henceforth, the priority regarding data privacy and security are solving a barrier to the broader the upgrade of cloud computing services. Data Security must be imposed on data by using encryption strategies to understand secured data storage and access. The cloud infrastructure is even more reliable and powerful than personal computing, but an oversized range of internal, external threats for data stored. Since the information don't seem to be stored within the client area, implementing security measures can't be applied directly. During this work, the RSA algorithm is implemented before storing sensitive data within the cloud. [1] When the authorized user requests the information for usage then data decrypted and provided to the user. In this paper, a way for Cloud ADPS by providing data storage and securing Cloud automatic processing system using RSA algorithm [8] and some important security services including key generation, encryption and decryption are provided in Cloud automatic data processing has been proposed.

II. Cloud Computing

Cloud computing is an emerging paradigm, which mainly concentrates to supply dynamic, on-demand scalability of virtualized recourse to line of users. Scalability and virtualization are the two key factors

of the cloud environment. because of the accessibility of the cloud computing services many researchers are focus on this area.

III. Cloud Architecture and Storage Architecture—

- A. *Cloud Architecture*: It typically involves multiple cloud components communicating with one another over application programming interfaces, usually web services. This is reverted to the clients where cloud applications can be accessed by software applications or web.
- B. *Cloud Storage Architecture*: High-level architecture description of cloud data storage services illustrated in Fig. 1. The architecture consists of 4 different entities: data owner, user, cloud server (CS), and Third-party Auditor (TPA)^[7]. The access of cloud storage security behalf of user, TPA is the trusted entity.

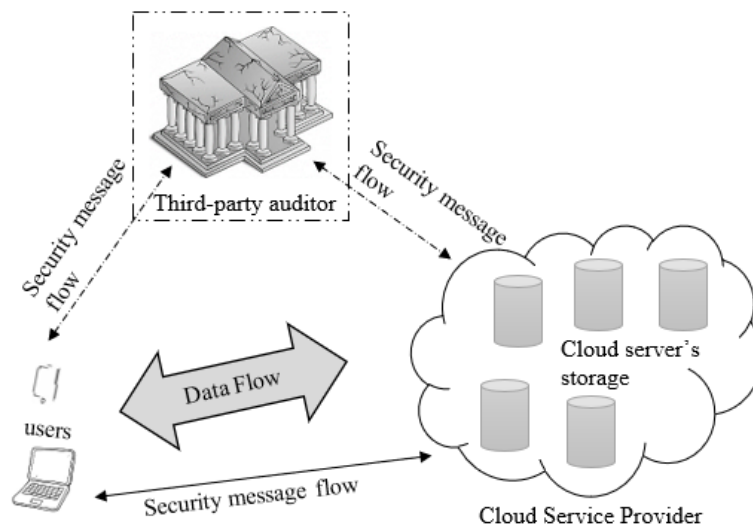


Fig. 1. The given is a sample model of cloud architecture which defines a cloud storage and infrastructure being using its services and the flow of data through the servers.

IV. Cloud Computing Service and Deployment Models

a. Service Models

Cloud computing separated into three service categories:

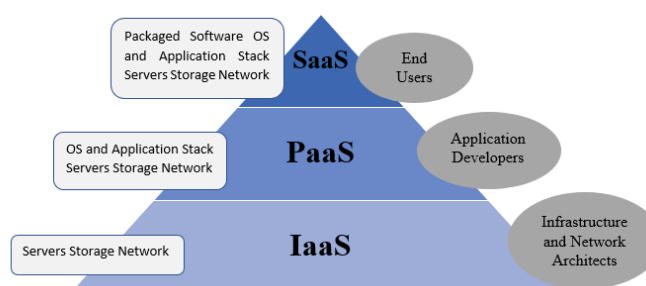


Fig. 2. The given is the service model description of cloud and their application.

Infrastructure as a service (IaaS) is a part of cloud computing resources that is virtualized. The hardware, software, servers, storage and other infrastructure components in IaaS are being hosted by a third-party provider on behalf of their users. Users' applications are also being provided by IaaS and handles tasks covering system maintenance backup and resiliency planning. IAAS platforms offer

highly scalable resources that can be adjusted on-demand to make it working for workloads that are temporary, experimental or changed unexpectedly. Other characteristics of IAAS environments covers dynamic scaling, desktop virtualization, the automation of administrative tasks and policy-based services. ^[3]

Platform as a service (PaaS) is also a cloud computing model that delivers applications. During a PaaS model, cloud provider delivers hardware and software tools i.e., being hosted by its own infrastructure. Actually, they are used for the application development as a service for users. Hence it leads to freeing PaaS users from putting in place in-house hardware and software to develop or run a replacement application. A PaaS provider, however, supports all the underlying computing and software; users only must login and start using the platform-usually through a web browser interface. ^[4] PaaS providers then charge for that access on a per-use basis or monthly basis.

Software as a service (SaaS) is a part of software distribution model from where applications are hosted by service provider and made available online for the customers ^[2]. SaaS has become an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new development approaches, like Ajax, become popular. SaaS is very similar to the ASP (Application service provider) and on-demand computing software delivery models. IDC identifies two minimal difference in delivery models for SaaS namely the hosted application model and so the software development model.

b. Deployment Models

- i. **Private cloud:** During this model cloud owner doesn't share their resources with the other organization. it's founded and maintained by a company. Security is often fine implemented during this model.
- ii. **Public cloud:** During this cloud model the resources are accessed by the final public. Everybody can access easily with this cloud so it's a less secure model. Cost of this cloud isn't expensive. This model requires a large investment these are owned by large organizations like Microsoft, Google or Amazon.
- iii. **Community cloud:** A cloud shares two or more several organizations or companies for his or her requirements. Usually employed in school or university campus.
- iv. **Hybrid cloud:** This sort of cloud uses one or more cloud model combinations for better use.

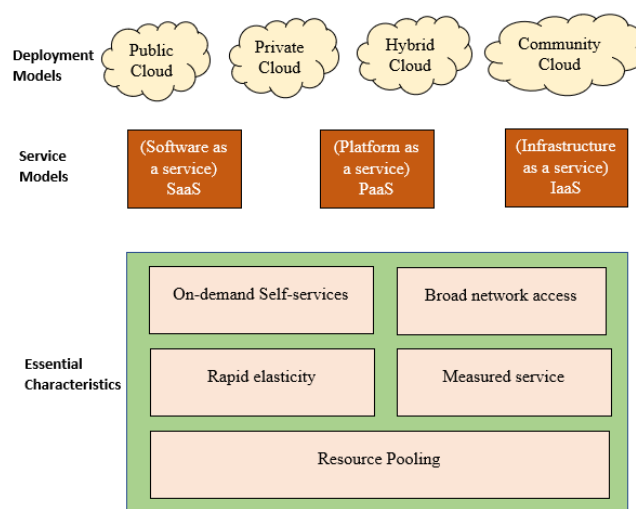


Fig. 3. Cloud model showing the composition of various service models and deployment models

V. The Proposed Methodology

The area of cryptography and cryptanalysis together are referred to as cryptology. Cryptanalysis used many encryptions and decryption techniques like Caesar cipher, Monoalphabetic cipher, Play fair cipher, Hill Cipher. These techniques possess the Brute Force Attack means the attacker tries every possible key to induce the first text to avoid this problem public key cryptography used. RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977.^[9]

In this proposed work, it is used for RSA algorithm to encrypt the information to produce security in order that only the concerned user can access it by securing the info as well as cipher.

RSA algorithm is that the public-key cryptography, within which both public and also the private keys are accustomed secure data within the cloud. the event of the general public key cryptography is greatest and maybe it provides a radical departure. it's also referred to as the Asymmetric algorithm because of the employment of two key together with a secret key. during this scheme, the plain text and cipher text are integers between 0 and $n-1$ for a few n . A typical size for n is 1024 bits.^[3]

RSA is a block cipher during which every message is mapped to an integer. RSA consists of Public-Key and Private-Key^[1]. In this Cloud environment, Pubic-Key is understood to any or all, whereas Private-Key and encrypted cipher key is thought only to the user who originally owns the info^[10]. Thus, encryption is finished by the Cloud service provider and decryption is finished by the Cloud user or consumer.

Once the information is encrypted with the Public-Key, it may be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

- Key Generation
- Encryption
- Decryption

Key generation: Before the information is encrypted Key generation should be done. This process is finished between the Cloud service provider and therefore the user.^[2]

Key generation algorithm Steps:

1. Choose two distinct prime numbers a and b . For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute $n = a * b$.
3. Compute Euler's totient function,
 $\phi(n) = (a-1) * (b-1)$.
4. Chose an integer e , such that $1 < e < \phi(n)$ and a greatest common divisor of e , $\phi(n)$ are 1.
Now, e is released as Public-Key exponent.
5. Now determine d as follows:
 $d = e^{-1} \pmod{\phi(n)}$ i.e., d is multiplicate inverse of $e \pmod{\phi(n)}$.
6. d is kept as Private-Key component, so that $d * e = 1 \pmod{\phi(n)}$.
7. The Public-Key consists of modulus n and the public exponent e i.e., (e, n) .
8. The Private-Key consists of modulus n and the private exponent d , which must be kept secret i.e., (d, n) .

Encryption algorithm: Encryption is the process of converting original plain text (data) into cipher text (data).^[9]

Steps:

1. The cloud service provider should give or transmit the Public- Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed-upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text(data) C is $C = m^e \pmod n$.
4. This cipher text or encrypted data is now encrypted again with the key (n, e) and being stored with the Cloud service provider.

Decryption algorithm:

Decryption is the process of converting the cipher text(data) to the original plain text(data).^[3]

Steps:

1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted cipher i.e., cipher.
3. The Cloud user then decrypts the cipher using values (d, n) first and hence the data by computing, $m = C^d \pmod n$.
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

VI. Experimental results and analysis

One of the experimental results shown here with the sequence of sections.

Key generation part:

The first part of key generation is to encrypt the original message into some integral byte code.

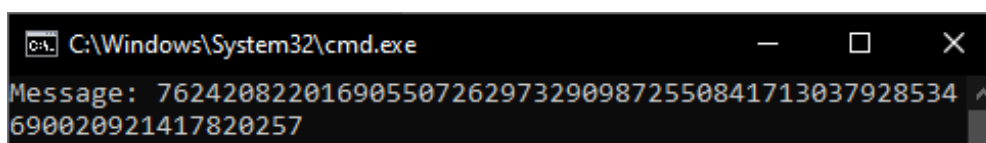


Fig. 4. Encrypted data

After the encryption of the message, two prime numbers are being chosen randomly to avoid the complication of attacking. Once the prime number is selected, $p1*p2$ is calculated according to the algorithm of RSA. Hence Euler's Totient is computed.

```

C:\Windows\System32\cmd.exe
Prime 1: 234995258392607899146206684800862555103577175246250559007670352166639495188512950235197627975794344225900464323
820779087513531140184630554302282695255500231479314049919307538493642253122835546019560332969189367518573625143988650116
14728061893925567735975379824321498940117735663115537148345351331152312885798327755472047901026231791066051919766305038
48875925600628200648866053216561478957235068611517774707659391339820496664050105552021509736202610149185980236438016024
74155302922297975497525916055645487317081840810384473332282641245275504437963639060154515379444277222766068737340750479
0633338754525714918111107

Prime 2: 186580410975925804921093864090996654234489822098410388692303879236591762968656710619277920010321170227116786657
664685626488209166963966088757999361285261686572057017648561585869989246682230648332922103693682601867022655906469290415
483942083313344266414935449444108278757809433375283382596419337757946425818677311937006535299419064297067385046294059550
036373116227817879463316147598035235606489664046901127321119399205962997317787740040749066750006407506715253185175139864
900482526483948528096782356234675009639400987240506961339255169277252797274284213878940666128632655781468345291163682369
41962691573017120604885833

phi p1 * p2: 43845511888286659491384195421807797435527940543623571919057157803611471775863472928302874388758671539593681
620881723026432683931251042999214008303586696442469743222563112181939037267749363707155758233441168371105215515191470549
036447022212745344860936446124696394154484745438606058697019567490311142691408489397770128551177039001511424973155150374
74807163703492198423641881037714818025643119852985372430566916392084336075158417667266263525852334682220796195539967955
907725023826995078484040808683031664985540117304454392202916509947825942661822159583161655794356282223113623059956545455
735853314279230695928782429651198132316834777391653319013841911251930525832310221909276825643291780332140124395911545060
686686696534140347555627630642305281007934385968742547452897395325198204399095267503846969815176784022655869981215483494
16502039449810513933938669168430445654859494732227701059811750180197322337001828634728927712093831559032086707707222463
777382341231272210442060888406860739732468119458989117911279951281327427593074999797271308715905817824390644357386823795
187011342196392996442833853439832446927328819594239541621832855098666747576736744403610821633867325315621772971379419158
8274388872941252637785458756873771168221250192

p1 * p2: 438455118882866594913841954218077974355279405436235719190571578036114717758634729283028743887586715395936816208
817230264326839312510429992140083035866964424697432225631121819390372677493637071557582334411683711052155151914705490364
470222127453448609364461246963941544847454386060586970195674903111426914084893977701285511770390015114249731551503747480
71637034921984236418810377148180256431198529853724305669163920843360751584176672662635258523346822207961955399679559077
250238269950784840408086830316649855401173044543922029165099478259426618221595831616557943562822231136230599565454557358
533142792306959287824296554138890105201144323263245027605033453111958057568313862765679573240929137118210044563005405478
41841064312857370482277823226840794203523993453680183050145057119150747739587474832848132274459661806943478442031880209
832050026845446556989187068304559863418397991502432797073697020376109108170148579839726677049214872456529090766754246587
167108918758563273122121292017385919878862566256181630683547829482163370521329233129883857241962803183501222489139717460
2367641252455339254208996071297580492347621508404499350490521102645233575602209109000504065313604266311706101734388697
830275791695922633754836021314003744247131

```

Fig. 5. Generation of random prime numbers and calculating values for keys

Encryption part:

The generation of public key and private key from the cipher generated by encrypting message. These keys emerged from the prime numbers chosen and the value generated as e, n, d .

```

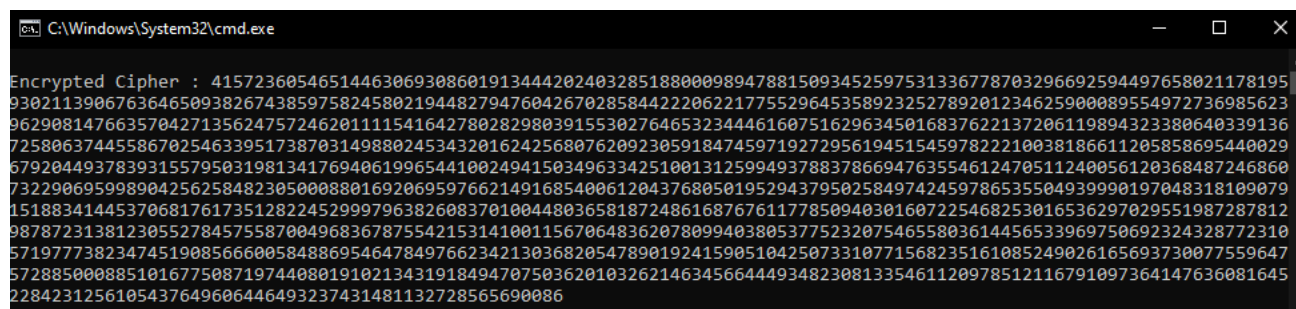
C:\Windows\System32\cmd.exe
Public key: 330450994409503340321063295179837597172105570428191690783408943226990364560813307278231778706324636651466636
161485807654169604607872664995793168069775506311747894616344590767656539347668123443046285009136388402475326025288784340
06646930308386525429807782215749623854444839799452529040178402025286843185472010610296133180814949424885774995150063057
095751914562236365474510084993932581651975519064117812304712214374087933000000134903487976148834285457432026779035399797
673180258205195250737150615125010352031316742916529744024645600984780443865723526417414316194993154685655349276513010896
381026583067822250850845709238989160728610653595778251715084048029745471330149396936206727987662419248798363320774849056
918128335379804126006650779563978750805997705704290281191096986796280840761036345591081392452586118883867255302209524387
611931880617819645613745673539087636977954720703298226825694749209673835199365000439204417379374088743927262085684482147
670470761725383587397044785213145490405599044116909448114713417325242141948981226758471629847787881200952274631656022249
739371182492645538892886246852863975587204294204675559643344983671219223325953201892425659005076082001703437768303877596
576654514839561072850460904094913199739043259

Private key: 19251514374401362529879238848382932470017423081402162883491135187200066320933806089691990469725795004469878
632465382416504661847954010290822305742452493348692169273963205539047224465876899326903108262221912006497394520709375195
015795215654227537066615730473433609642803358942017597294148972574348494368169303084181626880238465414475742471162939701
187771657075362078864612533334818319139368353827660591796226787865058468216890363154324170805643727178423996049692303706
862029906233958498960585087125840641175059673124003300142422944116641881731116151068521681467655997761379549790887961345
01296196673829571254357689193083813807978978863460026882436137549640387086869785238262897034626546517103954066283759093
937254493885697051218038528063040372350404002414899767383919811593984056482214639450072645659523443846426972160911999934
484572750483947265882444128573853543800914589852230915548913954958061291039451131173893087271831410218685242986011353201
246741904315621059789051632155259813675456736158308386102516628445993002747965727657895190005546067449247365765640132071
552045383804980438749146194966183485441889953773270851339183339451810644910904128221002897897196855365579145974875290289
5746092310109731108966422475110384869277240259

```

Fig. 6. Generated private and public key component

The encrypted cipher which is being used further in decryption part for the decryption of the cipher so that the original data can be retrieved.



```

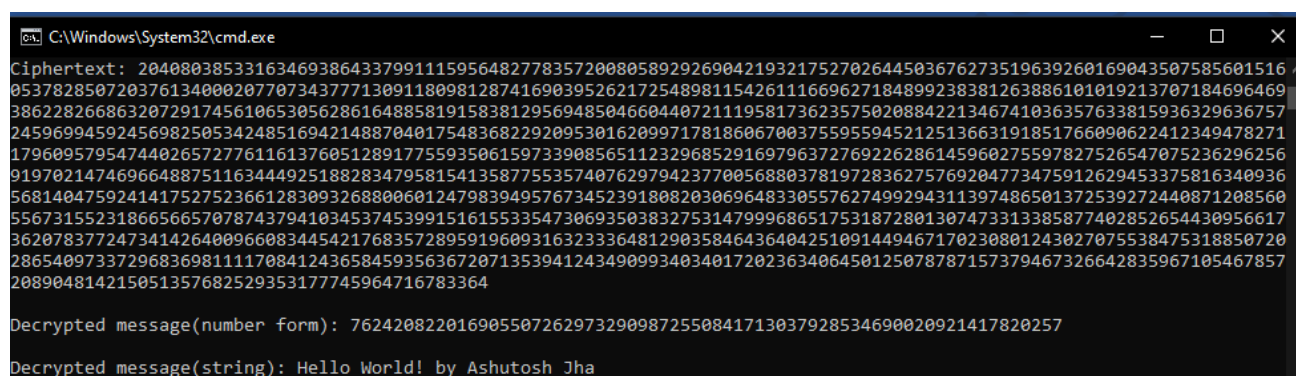
C:\Windows\System32\cmd.exe

Encrypted Cipher : 41572360546514463069308601913444202403285188000989478815093452597531336778703296692594497658021178195
930211390676364650938267438597582458021944827947604267028584422206221775529645358923252789201234625900089554972736985623
96290814766357042713562475724620111541642780282980391553027646532344461607516296345016837622137206119894323380640339136
725806374455867025463395173870314988024534320162425680762092305918474597192729561945154597822210038186611205858695440029
679204493783931557950319813417694061996544100249415034963342510013125994937883786694763554612470511240056120368487246860
732290695998904256258482305000880169206959766214916854006120437680501952943795025849742459786535504939990197048318109079
151883414453706817617351282245299979638260837010044803658187248616876761177850940301607225468253016536297029551987287812
987872313812305527845755870049683678755421531410011567064836207809940380537752320754655803614456533969750692324328772310
571977738234745190856660058488695464784976623421303682054789019241590510425073310771568235161085249026165693730077559647
572885000885101677508719744080191021343191849470750362010326214634566444934823081335461120978512116791097364147636081645
2284231256105437649060446493237431481132728565690086
  
```

Fig. 7. Encrypted Cipher

Decryption part:

Finally, the data is being decrypted using the key and the cipher text.



```

C:\Windows\System32\cmd.exe

Ciphertext: 204080385331634693864337991115956482778357200805892926904219321752702644503676273519639260169043507585601516
053782850720376134000207707343777130911809812874169039526217254898115426111669627184899238381263886101019213707184696469
386228266863207291745610653056286164885819158381295694850466044072111958173623575020884221346741036357633815936329636757
24596994592456982505342485169421488704017548368229209530162099717818067003755955945212513663191851766090622412349478271
179609579547440265727761161376051289177559350615973390856511232968529169796372769226286145960275597827526547075236296256
919702147469664887511634449251882834795815413587755357407629794237700568803781972836275769204773475912629453375816340936
568140475924141752752366128309326880060124798394957673452391808203069648330557627499294311397486501372539272440871208560
556731552318665665707874379410345374539915161553354730693503832753147999686517531872801307473313385877402852654430956617
362078377247341426400966083445421768357289591960931632333648129035846436404251091449467170230801243027075538475318850720
286540973372968369811117084124365845935636720713539412434909934034017202363406450125078787157379467326642835967105467857
208904814215051357682529353177745964716783364

Decrypted message(number form): 7624208220169055072629732909872550841713037928534690020921417820257
Decrypted message(string): Hello World! by Ashutosh Jha
  
```

Fig. 8. Decrypted cipher text and hence the data decrypted

VII. Conclusion

Cloud Computing remains a replacement and evolving paradigm where computing is thought to be on-demand service. Once the organization decides to maneuver to the cloud, it loses control over the info. Thus, the quantity of protection needed to secure data is directly proportional to the worth of the information. Cloud Security basically depends on the trusted computing and cryptography. Thus, in this proposed work, only the authorized user can access the information. whether or not some intruder (unauthorized user) gets the info accidentally or intentionally if he/she captures the info also, he/she can't decrypt it and obtain back the initial data from it. Henceforth, data security is provided by implementing the RSA algorithm. In this work, performance supported different parameters like space complexity, time complexity and throughput has been observed. we've got observed each efficiency parameter intimately by varying message packet length and a non-public key length of our encryption scheme. On viewing the results, it good to say that the RSA encryption algorithm is a feasible solution for secure communication in cloud computing.

References—

- [1] Shreya Srivastav, Shalika “Improving data security in cloud computing by using RSA and Digital Signature Algorithm “A special issue of IJTR(ISSN 2278-5787) SERB sponsored two day national conference on “ Current trends in scientific research for engineering applications (NCCSE-2015)” dated march 20-21, 2015
- [2] P.suresh “Secure Cloud Environment Using Rsa Algorithm”, International Journal of Computer Science and Information Technology, e-ISSN: 2395 -0056, p-ISSN: 2395-0072, Volume: 03 Issue: 02 | Feb-2016
- [3] Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R.K. Tiwari, “Data Security using RSA Algorithm in Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering, ISSN (Online) 2278-1021, Vol. 5, Issue 8, August 2016.
- [4] Sudhansu Ranjan Lenka, Biswaranjan Nayak, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014
- [5] Dr. Rajamohan Parthasarathy, Ms. Haw Wai Yee P, Mr. Seow Soon Loong, Dr. Leelavathi Rajamanickam, Ms. Preethy Ayyappan, IJSET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 4, April 2019, ISSN (Online) 2348 – 7968
- [6] Dhaval Jha Vishva Tanna Ripal Patel, " Data Security in Cloud using RSA" - International Journal for Scientific Research & Development| Vol. 2, Issue 04, 2014 | ISSN (online): 2321-0613
- [7] Shreya Srivastav, Neeraj Verma, M. Tech Scholar, Department of CSE, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 7, July 2015
- [8] Ms. Soumya.N.S, Mrs. Prabha.R, M.Tech Student, Computer Network Engineering, Associate Professor, Department of Information Technology, Volume IV, Issue X, October 2015 IJLTEMAS ISSN 2278 – 2540
- [9] Nasrin Khanezaei, Zurina Mohd Hanapi, “A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services”, IEEE, 58-62, 2014.
- [10] Balkees Mohamed Shereek, ZaitonMuda, SharifahYasin, Faculty of computer science and information technology, IOSR Journal of Engineering (IOSRJEN)ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 04, Issue 02 (February. 2014), ||V6|| PP 01-08